BÜNDNIS 90/DIE GRÜNEN, Adolfstr. 67, 65307 Bad Schwalbach

Herrn Kreistagsvorsitzenden
André Stolz
Heimbacher Str.7
65307 Bad Schwalbach

Kreistagsfraktion
Adolfstr. 67
65307 Bad Schwalbach
✆ 06124 / 720 060
gruene-rtk-fr@online.de

Bad Schwalbach, den 14.12.2021

46/21

fr 14/12/21

Dringlichkeitsantrag: IT-Sicherheit vor dem Hintergrund von Log4J

Sehr geehrter Herr Kreistagsvorsitzender Stolz,

bitte nehmen Sie den nachstehenden Dringlichkeitsantrag mit auf die Tagesordnung der nächsten Kreistagssitzung.

Mit freundlichen Grüßen

Günter Linke

Günter Linke
Fraktionsvorsitzender

Antragstext:
Die vom Kreistag in der Sitzung am 21. September 2021 beschlossenen externen Pentests in Bereichen kritischer Infrastruktur sollen schnellstmöglich durchgeführt werden.

Insbesondere soll überprüft werden, ob Server-Systeme mit Log4J (bspw. Apache) verwendet werden, die von einer schwerwiegenden Sicherheitslücke betroffen sind.

Begründung:
Aus dem aktuellen Bericht des Landrats vom 14. Dezember 2021 geht hervor, dass die Überprüfungen der IT-Sicherheit in Bereichen kritischer Infrastruktur vorerst nicht erfolgen soll. Dies wird mit fehlenden personellen Ressourcen begründet. Da die Pentests extern durchgeführt werden sollen, ist dieses Argument wenig einleuchtend. In Anbetracht der Beauftragung externer Dienstleister ist sowieso nicht mit einer kurzfristigen Einbindung des Personals des Gesundheitsamts zu rechnen.

Gerade jetzt – angesichts hoher Infektionszahlen – ist es wichtig, dass die IT-Infrastruktur sicher ist. Die Gesundheitsämter müssen funktionstüchtig bleiben.

Am Wochenende hat zudem das BSI mit der Meldung CVE-2021-44228[1] die höchste Warnstufe „rot" ausgerufen. Dieses bedeutet: „Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden." Hintergrund ist eine schwerwiegende Sicherheitslücke im Java-Framework Log4J, die Millionen an Servern für die Ausführung arbiträren Codes anfällig macht. Das BSI bestätigte zuletzt, dass diese Lücke bereits kriminell ausgenutzt wird (u. a. zum Cryptomining) und Hacker*innen sogenannte „Backdoors" (engl. Hintertüren) einbauen, um bspw. zu späteren Zeitpunkten Ransomware-Angriffe durchzuführen.[2] Genau dieser Angriffsvektor wurde in der Begründung unseres Antrags auf externe Pentests skizziert. Die Sicherheit der IT darf gerade jetzt nicht hintangestellt werden.

[1] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3
[2] https://www.tagesschau.de/inland/bsi-schadsoftware-103.html